Testimony of

John Milazzo

President/CEO of Campus Federal Credit Union

On behalf of

The National Association of Federal Credit Unions

"Data Security: Small Business Perspectives"

Before the

House Small Business Committee

Subcommittee on Finance and Tax

United States House of Representatives

June 6, 2007

National Association of Federal Credit Unions
3138 10th St. North
Arlington, VA 22201
(703) 522-4770
www.nafcu.org

Introduction

The National Association of Federal Credit Unions (NAFCU) is the only national organization exclusively representing the interests of the nation's federally chartered credit unions. NAFCU is comprised of over 800 federal credit unions—member owned financial institutions across the nation—representing more than 27 million individual credit union members. NAFCU–member credit unions collectively account for approximately two-thirds of the assets of all federal credit unions. NAFCU and the entire credit union community appreciate the opportunity to participate in this hearing regarding data security.

Historically, credit unions have served a unique function in the delivery of necessary financial services to Americans. Established by an act of Congress in 1934, the federal credit union system was created and has been recognized as a way to promote thrift and to make financial services available to all Americans, many of whom would otherwise have no access to financial services. Congress established credit unions as an alternative to banks and to fill a precise public need—a niche that credit unions continue to fill today for over 89 million Americans. Every credit union is a cooperative institution organized "for the purpose of promoting thrift among its members and creating a source of credit for provident or productive purposes." (12 USC 1752(1)). While over 70 years have passed since the *Federal Credit Union Act* (FCUA) was signed into law, two fundamental principles regarding the operation of credit unions remain every bit as important today as in 1934:

- Credit unions remain totally committed to providing their members with efficient, low cost personal service; and,
- Credit unions continue to emphasize traditional cooperative values such as democracy and volunteerism.

Credit unions are not banks. The nation's 8,305 federally insured credit unions serve a different purpose and have a fundamentally different structure, existing solely for the purpose of providing financial services to their members. As owners of cooperative financial institutions united by a common bond, all credit union members have an equal say in the operation of their credit union—"one member, one vote"—regardless of the dollar amount they have on account. These singular rights extend all the way from making basic operating decisions to electing the board of directors—something unheard of among for-profit, stock-owned banks. Unlike their counterparts at banks and thrifts, federal credit union directors generally serve without remuneration—a fact epitomizing the true "volunteer spirit" permeating the credit union community.

Credit unions have an unparalleled safety and soundness record. Unlike banks and thrifts, credit unions have never cost the American taxpayer a single dime. While the Federal Deposit Insurance Corporation (FDIC) and the Federal Savings and Loans Insurance Corporation (FSLIC) were both started with seed money from the United States Treasury, every dollar that has ever gone into the National Credit Union Share Insurance Fund (NCUSIF) has come from the credit unions it insures. Furthermore,

unlike the thrift insurance fund that unfortunately cost hundreds of billions of dollars, credit unions have never needed a federal bailout.

I am currently the President and CEO of Campus Federal Credit Union, headquartered in Baton Rouge, Louisiana. I am testifying today on behalf of the National Association of Federal Credit Unions, where I serve as the Chairman of its Board of Directors. Campus FCU Union has $332 million in assets and more than 37,000 members. Campus FCU is one of the oldest credit unions in the United States. It was formed in 1934 by ten employees of Louisiana State University and was issued charter number 79.

I have nearly forty years of experience in the financial services industry, having worked for several Louisiana banks before joining Campus Federal Credit Union as President and CEO in 1985. I have also served on the Federal Reserve Bank of Atlanta's Financial Institutions Advisory Committee. Additionally, I am the past Chair of the Southern Financial Exchange, a regional automated clearinghouse association. I also serve as a member of the Advisory Board for XP Systems, a leading computer software developer. In 2005, I was appointed to the Fannie Mae National Advisory Council. Finally, I currently serve as the Chair of the Finance Committee of Saint Anne's Catholic Church.

The Data Security Problem

As the members of this subcommittee well know, data breaches are a significant problem for both consumers and businesses. The number and breadth of data breaches are so great that it is difficult to calculate losses incurred to both the consumer and financial institution as a result of compromised data with any sort of specificity. The Federal Trade Commission (FTC) estimates the cost to be in the millions of dollars each year for new account losses when circumstances such as a criminal opening up a credit card account in a victim's name occur. While a comprehensive figure is difficult to determine, I can tell you that data breaches have cost Campus FCU and our member owners a significant amount of money.

Looking to a few high profile examples, the TJX data breach has already cost Campus FCU over $11,000. When Credit Card Systems Solutions suffered a breach, Campus FCU spent over $20,000 total to issue new cards and respond to our members' concerns, and this does not include the credibility and reputation issues that are discussed below.

In 2006, Campus charged off just under $50,000 in fraud losses on our debit cards. Additionally, Campus charged off over $130,000 in other fraud stemming from forgery, skimmed account numbers and stolen cards. Additionally, the cost of insurance for credit and debit cards is increasing dramatically. In the last six years Campus' premiums for payment card fraud coverage have increased by more than 64 percent. At

the same time, Campus' deductible for payment (credit & debit) card losses has also increased significantly. From 2001 to 2004, our deductible for payment card fraud and forgeries averaged $100. Today, our deductible is $1,500, an increase of 1,400 percent over six years.

Campus FCU's situation is not unique among the credit union community or the financial services industry as a whole. Analysis has shown that credit unions incurred over $100 million in payment card fraud in each of the last two years. Although it varies by institution, the cost associated with reissuing ATM and debit cards can run as high as ten dollars or more, costs that the 89 million Americans who are credit union members ultimately pay.

Dealing with potential data security issues is an issue that many credit unions are spending more and more time on in recent years. For example, when Campus is notified of a data breach impacting credit cards, we follow a 16-step flow chart, that includes at least 2 methods of notification to our members. We also keep enough credit card stock in house to cover at least 15% of our credit card base, allowing us to reissue cards in a very timely manner.

In addition to the cost credit unions and other financial institutions incur in notifying consumers, issuing new cards, changing account numbers, etc., there is also considerable cost, both in money and time, for consumers. Those that must have their cards re-issued may face the inconvenience of losing access to their credit or debit cards

for a period of time. If that member were a small business who needed to use those cards on a daily basis, their business could be impacted as well. Furthermore, although an individual whose identity has been stolen many not necessarily incur large out of pocket expenses, they may find the process of repairing identity theft and restoring credit a very time consuming ordeal.

There can be added costs in the form of credit monitoring services for those who are dedicated to ensuring they do restore their credit and don't become repeat victims. The victim may also request several credit reports each year from the three major credit reporting agencies in order to ensure that there is no unauthorized activity taking place in their name. When a credit union member is a victim of identity theft, the credit union oftentimes will work with them and help them monitor their credit union account.

Protecting Consumer Information

NAFCU supports efforts to enact a comprehensive proposal to protect consumers' personal data. Credit unions and other financial institutions already protect data consistent with the provisions of the Gramm-Leach-Bliley Act (GLB). There is no comprehensive regulatory structure similar to GLB for retailers, merchants or others who collect or hold sensitive personal information. While NAFCU supports new measures to combat data breaches, any new legislation should create a safe harbor for financial institutions already in compliance with GLB; failing to do so would place an undue burden and cost on financial institutions that would be forced to retool systems that they already have in place.

Consistent with Section 501 of GLB, the National Credit Union Administration (NCUA) established administrative, technical and physical safeguards (1) to ensure the security, (2) confidentiality, (3) integrity, (4) and proper disposal of consumer information and other records. Under the rules promulgated by the NCUA, every credit union must develop and maintain an information security program to protect customer data. Additionally, the rules require that third party service providers that have access to credit union data take appropriate steps to protect the security and confidentiality of the information.

GLB and its implementing regulations have successfully limited data breaches among financial institutions. The best way to move forward and address data breaches is to create a comprehensive regulatory scheme for those industries that are not already subject to oversight. At the same time, the oversight of credit unions, banks and other financial institutions is best left to the functional financial institution regulators that have experience in this field. By and large, financial institutions have not been the source of significant data breaches. It would be redundant at best and possibly counter-productive to authorize any agency - other than the functional financial institution regulators - to promulgate new, and possibly duplicate or contradictory, data security regulations for financial institutions already in compliance with GLB.

Accountability for Those Who Do Not Protect Consumer Information

The burden of addressing a data breach should fall on the entity responsible for the breach. Under the current law, some institutions and industries do not have a strong enough incentive for protecting sensitive information, as evidenced by the widespread number of data breaches that have been reported over the last several years.

There are two motivating factors as to why those who collect and hold sensitive information do not do enough to protect it. First, the cost associated with the data breach often falls on others. Second, because others – for example a financial institution issuing the payment cards with new numbers – generally have to repair the problems caused by a data breach, consumers often incorrectly assume that these institutions were responsible for the breach. The first notification that they get that their information may be compromised is often a call or letter from their credit union. By looking out and taking care of their members, credit unions (and other financial institutions) can unintentionally suffer some ill will from a member who finds out that their payment card from that institution has been re-issued. Thus the companies responsible for the data breach in the first place oftentimes do not suffer any loss of customer goodwill, at the same time consumer confidence in financial institutions, such as credit unions, may suffer.

While, the reputation risk to financial institutions may be difficult to solve with legislation, Congress should consider holding accountable those companies that are responsible for significant data breaches. Obviously, data breaches are going to continue

to be a fact of life for any company that holds personal information. Unfortunately, no matter how quickly government and industry reacts, criminals will always find new and inventive ways around security measures. Even with everything that financial institutions and other parties can do to protect data, it is important that there be stiff penalties and full enforcement of the laws that prohibit and punish the actual crooks who take the action to commit these breaches by stealing, and often selling or using this compromised data.

Nonetheless, any data security bill should place the burden of addressing a data breach on the entity responsible for the breach, whether it is the financial institution, retailer, data broker, or any other third party. The entity at fault that did not adequately protect the data in accordance with best practices and the law should be responsible for all direct costs associated with loss, including notifying regulators, law enforcement and credit bureaus, while covering the costs incurred by financial institutions in their efforts to protect consumers who have been affected by the security breach. It is not our intent to have data breaches put any company out of business. Instead, we believe that there must be a strong incentive for businesses to properly protect consumer's financial data, otherwise, as evidenced by recent instances of payment card breaches, the information may not be adequately protected and the credit union could end up being the one that pays.

It is with this in mind that NAFCU believes it is important that any bill approved by Congress include language to reimburse, in a timely manner, impacted financial institutions for the direct cost that they incur due to a data security breach that was no

fault of their own. While some may believe that interchange fees are designed to address this issue, the true intent of interchange fees was to meet the costs of the credit processing system (including limited fraud) and not to cover the impact of major breaches and the costs associated with the failure to adequately protect data. Without additional federal incentive to comply and protect data, any legislation that does not increase the burden on responsible parties could end up being a paper tiger. Current data security standards with payment card companies such as Visa and Mastercard prohibit storing sensitive data and even impose fines for those that do, yet, either because the penalties are not harsh enough or the contracts aren't enforced, data ends up being stored and breaches still end up happening. Some states, such as Minnesota recently, have enacted tougher standards to hold those responsible accountable. We believe any federal data security bill needs to do the same.

Finally, it should be noted that financial losses to credit unions are especially troubling, because unlike banks and other financial institutions, credit unions do not make profits for shareholders, do not issue stock and aren't able to turn to capital markets for money to make up for data breach losses. All monies at a credit union must be raised through their members. Financial losses to the credit union are ultimately passed back to the member in the form of either reduced services, lower dividends on savings, higher interest rates on loans (either personal or business), or even decreased availability of loans.

As mentioned above, financial institutions often suffer the loss of goodwill as consumers often think their credit union or bank is responsible for the breach because they must re-issue plastic, change account numbers, etc. However, financial institutions are rarely the source of a data breach. Merchants, data brokers and others, however, have been shown to have kept records of their customers' financial account information without adequately protecting it. As such, NAFCU supports placing the financial burden for repairing the damages associated with a data breach on the entity responsible.

Conclusion

NAFCU supports new measures to ensure industry takes adequate steps to protect consumers' sensitive financial data. The most efficient way to address the growing number of data breaches is to create a comprehensive regulatory scheme for those entities that currently have none. NAFCU believes that a safe harbor for financial institutions already in compliance with section 501 (b) of Title V of the *Gramm-Leach- Bliley Act* (GLBA) should be included in any data security bill. Further, if more regulations are needed to address new concerns, it should be the functional regulators that are charged with promulgating new rules. Finally, merchants, retailers, data brokers or any other party that holds customer information should be held financially accountable if it is responsible for a data breach.